Szczegółowy opis przedmiotu zamówienia

I. Zakres przedmiotu zamówienia obejmuje:

1. W zakresie architektury rozwiązania:
   1) opracowanie architektury rozwiązania uwzględniającej:
      a) plan adresacji,
      b) reguły konfiguracji urządzeń, w tym firewalli,
      c) schematy komunikacji wewnątrz systemu dla poszczególnych typów urządzeń objętych wdrożeniem;
   2) przedłożone opracowanie musi uzyskać akceptację Zamawiającego w terminie określonym w Umowie.
2. Opracowanie harmonogramu:
   1) opracowanie harmonogramu wdrożenia 10% agentów wg dostarczonej licencji oraz na podstawie zestawień udostępnionych przez Zamawiającego, uwzględniających liczbę komputerów wraz z ich podziałem na systemy operacyjne w poszczególnych jednostkach objętych wdrożeniem wg załącznika nr 2 do umowy. Wykonawca w uzgodnieniu z Zamawiającym wytypuje nie więcej niż 10 lokalizacji, w których przeprowadzone zostanie przeprowadzona instalacja agentów.
      Przedłożony harmonogram musi uzyskać akceptację Zamawiającego w terminie określonym w Umowie;
   2) harmonogram musi uwzględniać lokalizacje, terminy oraz liczby urządzeń podlegających wdrożeniu.
3. Dostarczenie licencji:
   1) dostarczenie wszystkich niezbędnych do funkcjonowania systemu licencji typu perpetual - wieczyste, potwierdzonych dokumentem licencyjnym producenta oprogramowania, a obejmujących stronę serwerową (w tym bazę danych, jeśli jest stosowana), licencje na agentów w sumarycznej liczbie co najmniej 10 000 szt., obejmujące systemy operacyjne Microsoft Windows, Linux, MacOS, iOS, Android użytkowane przez Zamawiającego;
   2) dopuszcza się nieograniczone licencjonowanie typu enterprise;
   3) Zamawiający nie dopuszcza licencjonowania opartego na subskrypcji.
4. Wdrożenie systemu:
   1) przeprowadzenie wdrożenia zgodnie z harmonogramem;
   2) instalacja agentów;
   3) konfiguracja i uruchomienie centralnego systemu zarządzania zgodnie z zaleceniami producenta oprogramowania i najlepszymi praktykami;

4) sprawdzenie poprawności funkcjonowania systemu dla wytypowanych jednostek Gminy Lublin, w szczególności:
   a) konsoli zarządzającej,
   b) automatycznej inwentaryzacji zasobów sprzętowych i oprogramowania,
   c) zdalnego dostępu,
   d) aktywności użytkowników,
   e) statystyk z użytkowania aplikacji,
   f) przypisywania licencji
   g) przygotowanie raportu zabronionych aplikacji,
   h) weryfikacji separacji dostępu do obiektów dla poszczególnych administratorów/operatorów,
   i) przeprowadzenie backupu i odtwarzania systemu,
   j) przeprowadzenie testów penetracyjnych obejmujących skanowanie portów, badanie podatności systemu operacyjnego oraz aplikacji na znane luki w bezpieczeństwie, weryfikację poprawności działania firewalla, ocenę poprawności reakcji systemu zabezpieczeń na wykonywane ataki DDOS, w tym co najmniej:
      - flooding,
      - smurfing,
      - IP fragmentation,
      - syn flood,
      - nuking.

   Testy kończą się pełnym raportem z przeprowadzonych czynności.
5) opracowanie dokumentacji powykonawczej obejmującej co najmniej:
   - schematy funkcjonalne rozwiązania,
   - opis architektury logicznej,
   - opis komponentów aplikacyjnych,
   - opis wykonanych czynności instalacyjnych oraz konfiguracyjnych wszystkich komponentów systemu,
   - listingi krytycznych plików konfiguracyjnych,
   - skryptów instalacyjnych,
   - konfigurację firewalli,
   - procedury eksploatacji, w tym instalacji, reinstalacji, aktualizacji systemu, konfiguracji systemu dla nowych jednostek,
   - procedury backupu i odtwarzania (w tym disaster recovery),
   - zalecenia bezpieczeństwa w zakresie bezpiecznej eksploatacji systemu, kontroli i monitorowania dostępu, w tym prób naruszenia zasad bezpieczeństwa.

5. świadczenie asysty technicznej:
   a) świadczenie asysty technicznej na rzecz Zamawiającego zgodnie z zapisami terminów Umowy, obejmującą:

- zapewnienie ciągłości działania systemu,
- wsparcie w zakresie wykrywania przyczyn awarii i niestabilnej pracy,
- obsługi błędów wszystkich elementów wdrożonego systemu,
- aktualizacji oprogramowania dostarczonego w ramach Umowy do najnowszej dostępnej i stabilnej wersji,
- optymalizacji systemu,
- przeprowadzania nieograniczonych konsultacji technicznych,

b) wszelkie zmiany w systemie skutkujące niedostępnością lub wpływające na jego stabilność lub wydajność wymagają uprzedniej zgody Zamawiającego.

Zgłoszenia w ramach asysty technicznej dokonywane będą w systemie zgłoszeń Wykonawcy lub za pośrednictwem poczty e-mail z potwierdzeniem otrzymania zgłoszenia, z terminem realizacji do ..... dni roboczych dla błędów krytycznych oraz z terminem realizacji 5 dni roboczych dla usterek, gdzie błąd krytyczny to sytuacja polegająca na nieprawidłowym, funkcjonowaniu systemu, w tym niezgodnie z dokumentacją, skutkująca:
- niedostępnością systemu,
- niespójnością danych
- zawieszaniem się systemu,
- niedostępnością funkcjonalności określonych w dokumentacji;

a usterka to sytuacja inna niż błąd krytyczny, polegająca na nieprawidłowym funkcjonowaniu systemu, nieograniczająca zakresu funkcjonalnego, lecz utrudniająca pracę użytkownikom lub administratorom.

6. przeprowadzenie analizy powdrożeniowej:

Wykonawca zgodnie z terminem określonym w Umowie zobowiązuje się przeprowadzić audyt systemu, dokonać jego optymalizacji z uwzględnieniem zwiększonej liczby agentów, zmian struktury sieci informatycznej Zamawiającego oraz jednostek organizacyjnych UM Lublin, dokonać aktualizacji dokumentacji powykonawczej.

7. przeprowadzenie szkoleń:

a) szkolenie podstawowe:

- przeprowadzenie podstawowych szkoleń z zakresu administracji, obsługi i utrzymania dostarczonego oprogramowania dla 100 administratorów wraz z udostępnieniem platformy elearningowej na potrzeby wdrożenia umożliwiającej przeprowadzenie testu końcowego uczestników z zakresu szkolenia,
- zakres szkolenia musi obejmować przygotowanie dedykowanej paczki instalacyjnej agenta na stację końcową, instalację/deinstalację agenta, analizę potencjalnych błędów (debugging), obsługę centralnej konsoli systemu w zakresie przyłączania agentów do odpowiedniej jednostki organizacyjnej, zdalnego dostę-

pu, rekonfiguracji stacji końcowej, nadawanie/odbieranie uprawnień, obsługi systemu zgłoszeń Wykonawcy,

- pozytywnie zweryfikowani uczestnicy szkolenia otrzymują dyplom potwierdzający zdobytą wiedzę i umiejętności z zakresu szkolenia;

b) szkolenie zaawansowane:

- przeprowadzenie zaawansowanych szkoleń dla 5 administratorów w zakresie niezbędnych funkcjonalności zapewniających sprawne zarządzanie środowiskiem skonfigurowanym do obsługi wielu jednostek, tworzenia własnych raportów, dostępu do bazy danych systemu, w tym budowania zaawansowanych zapytań bezpośrednio do bazy systemu, sposobów analizy logów, debbugowanie systemu, procedur bezpieczeństwa i zasad bezpiecznej eksploatacji,
- pozytywnie zweryfikowani uczestnicy szkolenia otrzymują dyplom potwierdzający zdobytą wiedzę i umiejętności z zakresu szkolenia.

II. Na potrzeby realizacji umowy Zamawiający dedykuje możliwość instalacji oprogramowania systemu zarządzania w środowisku VMware w wersji co najmniej 6.0 na serwerze HP Proliant BL 460c Gen9 o parametrach:

1) dwa procesory Intel Xeon E5-2680 v3;
2) 256GB RAM;
3) dwa dyski twarde 300GB skonfigurowane w RAID1;
4) karta Fibre Channel HP QMH2672 16Gb;
5) karta sieciowa HP FlexFabric 10Gb 2-port 536FLB Adapter;
6) przestrzeń dyskową z macierzy dyskowej HP 3PAR StoreServ 7400 zaprezentowaną czterema ścieżkami za pośrednictwem interfejsu Fibre Channel.

III. Powstały system wspierający inwentaryzację oraz zarządzanie stacjami roboczymi musi posiadać następujące cechy:

1. Oprogramowanie musi być w języku polskim.
2. Dostarczone licencje muszą być wieczyste (perpetual) i nie mogą podlegać subskrypcji.
3. System musi umożliwiać osadzenie w zwirtualizowanym środowisku Zamawiającego.
4. Architektura systemu musi być jednoinstancyjna, tzn. zapewniać dostęp do wszystkich zarządzanych przez system stacji roboczych w ramach pojedynczej, zintegrowanej konsoli administratorskiej (bez wymuszonego podziału na funkcjonalnie podobne podsystemy celem obsługi wszystkich objętych licencjonowaniem stacji roboczych). System musi zapewniać możliwość instalacji serwerów pomocniczych w zdalnych lokalizacjach zapewniając optymalną komunikację w ramach dystrybucji oprogramowania.
5. System musi umożliwiać współpracę z bazą typu OpenSource. Zamawiający dopuszcza możliwości korzystania z komercyjnego silnika bazy danych w przypadku, gdy jego instancja będzie dedykowana tylko na potrzeby wdrożenia, bez ponoszenia dodatkowych kosztów przez Zamawiającego.
6. System musi komunikować się ze stacjami roboczymi za pośrednictwem dedykowanego

agenta zapewniającego poufność przesyłanych informacji.

7. Obsługa konsoli musi umożliwiać zmianę kontrastu wyświetlanego obrazu oraz wielkość stosowanych czcionek ekranowych.
8. Interfejs konsoli musi być w całości dostępny z poziomu przeglądarki internetowej (Internet Explorer w wersji 10 lub nowszej, Mozilla 44 lub nowszej, Chrome 47 lub nowszej) bez potrzeby instalacji dedykowanego klienta. Dostęp do konsoli nie może wymagać korzystania z wtyczek w technologii Flash lub Java.
   Dopuszcza się wykorzystanie otwartej technologii HTML5.
9. Dla połączeń zdalnych system musi umożliwiać automatyczne wygaszanie ekranu użytkownika zdalnego, blokowanie klawiatury oraz myszki, widok w trybie tylko do podglądu.
10. System musi obsługiwać systemy operacyjne będące w posiadaniu Zamawiającego lub użytkowane przez jednostki Gminy Lublin w wersjach:
    1) Microsoft Windows XP, Vista, 7, 8, 10;
    2) Microsoft Server 2003, 2008R2, 2012R2, 2016;
    3) Linux CentOS 6.x, Debian 7.x, Ubuntu 10.x, RHEL 6.x;
    4) MacOS 10.13.x;
    5) Android 2.3;
    6) iOS 7.x;

    i nowszych.
11. System musi zapewniać równoczesny, zdalny, nieograniczony dostęp do konsoli dla co najmniej 100 administratorów/operatorów bez konieczności korzystania z technologii VPN
12. System musi mieć możliwość włączenia opcji uwierzytelniania dwuskładnikowego.
13. System musi zapewniać zarządzanie uprawnieniami operatorów na funkcjach systemu oraz dostępu do określonych zasobów (stacji roboczych, serwerów, urządzeń mobilnych).
14. System musi umożliwiać delegację uprawnień do określonych grup zasobów na podstawie uprzednio zdefiniowanych reguł (w szczególności typów zasobów, przypisanych lokalizacji, grup niestandardowych).
15. System musi umożliwiać zarządzanie użytkownikami z podziałem na funkcje administratora, audytora, gościa, managera zasobów, managera aktualizacji, z możliwością dodawania nowych ról z określonymi uprawnieniami.
16. System musi rozpoznawać stacje robocze z systemem Microsoft Windows w ramach Active Directory oraz Workgroup będącym w posiadaniu Zamawiającego.
17. System musi mieć możliwość dodania nowego użytkownika systemu z Active Directory
18. System musi umożliwiać generowanie następujących raportów na podstawie wbudowanych kryteriów w szczególności:
    1) aktywności użytkowników, w podziale na częstotliwość logowania, użytkowane stacje robocze;

2) w podziale na użytkowników w strukturze AD;

19. System musi posiadać moduł rozpoznawania i dodawania urządzeń:
    1) Ręcznego dodawania urządzeń;
    2) Dodawania urządzeń z pliku typu CSV;
    3) Uwierzytelnionego na podstawie poświadczeń użytkownika AD;
20. System musi mieć możliwość importu komputerów/stacji roboczych z Active Directory i dystrybucji agenta z poziomu konsoli.
21. System musi umożliwiać import i eksport danych.
22. System musi zapewniać automatyczny backup bazy danych i umożliwiać pełne odtworzenie tej bazy do czasu sprzed wystąpienia awarii.
23. System musi umożliwiać dystrybucję oprogramowania w formatach MSI, EXE lub poprzez skrypty.
24. System musi mieć wbudowane funkcje zarządzania i wdrażania aktualizacji na stacjach roboczych oraz serwerach, rozpoznawać sekwencje instalacji dla:
    1) systemów operacyjnych:
        a) Microsoft Windows: Vista, 7, 8, 10, 2003, 2008R2, 2012R2, 2016;
        b) Mac OS: X Server – Lion i nowszych;
        c) Linux: Ubuntu 14.04 LTS i nowszych, Debian 7 i nowszych; RHL/CenOS 6 i nowszych.
    2) oprogramowania:
        a) Windows: Microsoft Office, Microsoft Sharepoint, Google Chrome, Opera, Skype, Mozilla Firefox, Adobe Reader, Adobe Acrobat;
        b) MacOS: Adobe Reader, Adobe Acrobat, Mozilla Firefox, Google Chrome, Opera, Skype;
        c) Linux: Firefox;

    będących w posiadaniu Zamawiającego.
25. System musi mieć możliwość włączenia opcji testowania i zatwierdzania poprawek na wybranej grupie urządzeń przed instalacją poprawek w środowisku produkcyjnym.
26. System musi mieć wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące łaty systemowe.
27. System musi posiadać funkcję portalu samoobsługowego umożliwiającego użytkownikom instalowanie i uruchamianie oprogramowania z list aplikacji zatwierdzonych do użytku w jednostce.
28. System musi umożliwiać uruchamianie instalatora aplikacji z uprawnieniami dowolnego użytkownika.
29. System musi umożliwiać zarządzanie i rozliczanie licencjami aplikacji.
30. System musi umożliwiać wykrywanie zabronionego oprogramowania i uruchamiać zdefiniowane działania naprawcze.
31. System musi posiadać możliwość włączenia pomiaru wykorzystania wskazanej aplika-

cji.

32. System musi mieć możliwość blokowania plików wykonywalnych EXE poprzez reguły oparte na co najmniej na ścieżce dostępu do aplikacji lub wartości hash pliku.
33. System musi zapewniać możliwość dystrybucji agenta z wykorzystaniem mechanizmów Active Directory w ramach GPO.
34. System musi zapewniać poufność, a wymiana danych z agentami musi odbywać się w kanale szyfrowanym HTTPS
35. System musi zapewniać komunikację z agentami również poprzez połączenia NAT, bez potrzeby korzystania z technologii VPN.
36. System musi posiadać możliwość instalacji serwera pośredniczącego instalowanego w strefie DMZ, będącego dodatkową formą zabezpieczenie komunikacji pomiędzy serwerem aplikacji, a siecią zewnętrzną.
37. System musi zapewniać poprawną obsługę agentów w przypadku, gdy ich adresacja w różnych sieciach powtarza się.
38. System musi posiadać wbudowane narzędzia systemowe umożliwiające zdalne uruchomianie stacji roboczych, zdalne zamykanie stacji roboczych, skanowanie i czyszczenie dysków.
39. System musi posiadać wbudowane narzędzia zdalnego dostępu/wsparcia użytkownika, z opcją uzyskania zgody użytkownika na połączenie oraz możliwością nagrywania sesji.
40. System musi umożliwiać wdrażanie polityk konfiguracji dla systemów Windows, w szczególności polityk dostępu do interfejsu USB, zużycia energii, konfiguracji drukarek i przeglądarek internetowych.
41. Konfiguracja polityk dostępu do USB musi umożliwiać blokowanie no najmniej poniższych typów urządzeń, a także mieć możliwość wykluczania z listy zablokowanych konkretnych urządzeń o danym identyfikatorze urządzenia lub danego dostawcy, a dla dysków przenośnych na których dane są szyfrowane za pomocą wbudowanych narzędzi systemu Windows:
    1) mysz;
    2) stacja dysków (takie jak napędy USB, zewnętrzne dyski twarde oraz dyski wirtualne);
    3) cdrom;
    4) urządzenie przenośne: telefon, odtwarzacz multimedialny;
    5) dyskietka;
    6) bluetooth;
    7) typu obraz: kamera USB, skaner;
    8) drukarka;
    9) modem.
42. System musi umożliwiać przeprowadzanie prac serwisowych na stacjach roboczych z systemem Windows, bez potrzeby uruchamiania połączenia zdalnego typu RDP, co najmniej w zakresie:

1) podglądu, zamykania uruchomionych procesów na stacji roboczej;
2) podglądu, uruchamiania, zatrzymywania, zmiany stanu usług ;
3) uruchamianie zdalnego wiersza poleceń;
4) podgląd, dodawania i modyfikacji rejestru systemowego;
5) przeglądu logów systemowych;
6) podglądu menedżera urządzeń;
7) podglądu udziałów sieciowych;

43. System musi mieć rozpoznawać komponenty sprzętowe oraz oprogramowanie zainstalowane na stacjach roboczych.
44. System musi umożliwiać generowanie raportów na podstawie wbudowanych kryteriów w szczególności:
    1) aktywności użytkowników:
        a) w podziale na częstotliwość logowania;
        b) użytkowane stacje robocze;
        c) w podziale na użytkowników w strukturze AD.
    2) wykorzystania aplikacji w skali całej organizacji;
    3) aktualnego stanu oprogramowania i sprzętu z uwzględnieniem podziału:
        a) na oprogramowanie niedopuszczone do użytkowania;
        b) nielicencjonowane;
        c) liczby nowych stacji roboczych lub urządzeń mobilnych.
45. System musi rozpoznawać i indeksować popularne formaty multimedialne.
46. System musi mieć wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące aktualizacje systemowe.
47. System musi posiadać możliwość pomiaru wykorzystania określonej aplikacji.
48. System musi mieć moduł alarmujący o zmianach w dodawaniu/usuwaniu zasobów sprzętowych i oprogramowania na stacjach roboczych użytkowników oraz przechowywać historię tych zmian.
49. System musi umożliwiać wykonywanie zadań o określonym czasie oraz wysyłać powiadomienia e-mail o zmianach, które wystąpiły w systemie.
50. System musi umożliwiać ewidencjonowanie lokalnych kont z prawami administratora.
51. System musi posiadać moduł zarządzania bezpieczeństwem dla urządzeń mobilnych umożliwiający:
    1) zabezpieczenie przed nieautoryzowanym dostępem;
    2) zdalną blokadę, w przypadku utraty urządzenia;
    3) przeprowadzenie pełnego czyszczenia poprzez usunięcie wszystkich danych z telefonu w celu uniknięcia wycieku danych po kradzieży;
    4) tzw. organizacyjne czyszczenie poprzez usunięcie tylko danych organizacyjnych i pozostawienie danych prywatnych;
    5) szyfrowanie urządzenia;

6) ograniczanie użytkowania kamery, zainstalowanych aplikacji;
7) konfigurację ustawień polis dostępu do zasobów organizacyjnych.

52. System musi umożliwiać dołączanie załączników do wprowadzanych licencji, takich jak:
1) skany faktur;
2) klucze licencyjne;
3) dokumenty licencyjne.

53. System musi umożliwiać generowanie następujących raportów:
1) raporty z Active Directory:
   a) aktualnie zalogowani użytkownicy;
   b) często zalogowani użytkownicy/rzadko logujący się użytkownicy
   c) nieaktywni użytkownicy;
   d) historia logowania użytkownika;
   e) historia logowania użytkowników na poszczególnych komputerach;
   f) wykorzystania aplikacji w skali całej organizacji;
2) raporty dotyczące poprawek:
   a) narażone systemy;
   b) obsługiwane poprawki;
   c) brakujące poprawki czekające na zatwierdzenie;
   d) systemy wymagające ponownego uruchomienia;
3) raporty z inwentaryzacji sprzętu:
   a) komputery wg systemu operacyjnego;
   b) komputery wg producenta;
   c) komputery wg pamięci;
   d) komputery wg wykorzystania dysku;
   e) komputery wg wieku;
   f) komputery wg typu urządzenia;
   g) zamapowane dyski logiczne;
4) raporty z inwentaryzacji oprogramowania:
   a) oprogramowanie według producenta;
   b) ostatnio zainstalowane oprogramowanie;
   c) niedozwolone oprogramowanie;
   d) wykorzystanie oprogramowania przez komputer;
   e) klucze produktu oprogramowania;
   f) komputery z/bez określonego oprogramowania;
   g) podsumowanie zasad pomiaru użytkowania oprogramowania;
   h) oprogramowanie specyficzne dla użytkownika;
5) raporty licencji
   a) zgodność licencji;
   b) licencje do odnowienia;

6) raporty systemu:
   a) użytkownicy oraz grupy;
   b) komputery wg usług;
   c) szczegóły systemu;
7) raporty gwarancji
   a) o zbliżającym się terminie wygaśnięcia gwarancji;
   b) wygasłych gwarancjach;
   c) nieokreślonych gwarancjach;
8) raporty bezpieczeństwa:
   a) informacje o antywirusie;
   b) informacje o stanie szyfrowania;
   c) informacje o firewall;
9) raporty o plikach multimedialnych
   a) wg kategorii;
   b) wg rozszerzenia;
10) raporty z wykorzystania USB.

54. System musi umożliwiać tworzenie harmonogramów dla raportów i przesyłanie ich w formie pliku PDF, XLSX, CSV na wskazany adres mailowy.
55. System musi umożliwiać tworzenie niestandardowych raportów w oparciu o kryteria dostępne w systemie.
56. System musi umożliwiać tworzenie niestandardowych raportów w oparciu o wysyłanie zapytań do bazy danych z poziomu konsoli zarządzającej.
57. System musi mieć możliwość zdalnego instalowania i uruchamiania skryptów w formatach vb, js, ps1, cmd, msi, jse, exe, bat, vbe, vbs, wsf, wsc, wsh, reg, sh, scpt, pl, py, sh, bash, ksh, csh, tcsh.
58. System musi posiadać możliwość skanowania zasobów agenta bez połączenia z serwerem centralnym. Po wznowieniu tego połączenia musi przesyłać dane z ostatniego skanowania.
59. System musi zapewniać możliwość równoczesną obsługę kilku połączeń zdalnych przez tego samego administratora/operatora.
60. System musi umożliwiać przegląd nagranych sesji zdalnych oraz mieć możliwość ich eksportu.
61. System w ramach zdalnego wsparcia musi zapewniać transfer plików oraz chat z użytkownikiem.
62. System musi przechowywać historię zdalnych połączeń oraz komunikacji tekstowej pomiędzy administratorem a użytkownikiem, jeżeli taka komunikacja miała miejsce.
63. System w ramach zdalnego wsparcia musi zapewniać transfer plików oraz chat z użytkownikiem.
64. System musi mieć możliwość komunikacji pomiędzy użytkownikiem a administratorem

podczas sesji zdalnej w formie tekstowej, połączenia głosowego oraz video.

65. Dystrybucja agenta musi być realizowana w jednej z poniższych metod:

1) poprzez instalację agenta z poziomu konsoli programu w przypadku integracji systemu z usługą Active Directory;

2) poprzez instalację agenta za pomocą reguł GPO;

3) poprzez ręczną instalację agenta na każdej stacji roboczej.

DYREKTOR
Wydziału Informatyki i Telekomunik
Grzegorz Rudnicz